

ISC2

Exam Questions CCSP

Certified Cloud Security Professional



NEW QUESTION 1

Under EU law, a cloud customer who gives sensitive data to a cloud provider is still legally responsible for the damages resulting from a data breach caused by the provider; the EU would say that it is the cloud customer's fault for choosing the wrong provider.

This is an example of insufficient _____ .

- A. Proof
- B. Evidence
- C. Due diligence
- D. Application of reasonableness

Answer: C

NEW QUESTION 2

_____ can often be the result of inadvertent activity. Response:

- A. DDoS
- B. Phishing
- C. Sprawl
- D. Disasters

Answer: C

NEW QUESTION 3

What can tokenization be used for? Response:

- A. Encryption
- B. Compliance with PCI DSS
- C. Enhancing the user experience
- D. Giving management oversight to e-commerce functions

Answer: B

NEW QUESTION 4

DLP can be combined with what other security technology to enhance data controls? Response:

- A. DRM
- B. SIEM
- C. Kerberos
- D. Hypervisors

Answer: A

NEW QUESTION 5

Which cloud storage type uses an opaque value or descriptor to categorize and organize data? Response:

- A. Volume
- B. Object
- C. Structured
- D. Unstructured

Answer: D

NEW QUESTION 6

All of the following are usually nonfunctional requirements except _____.

Response:

- A. Color
- B. Sound
- C. Security
- D. Function

Answer: D

NEW QUESTION 7

The cloud deployment model that features organizational ownership of the hardware and infrastructure, and usage only by members of that organization, is known as:

Response:

- A. Private
- B. Public
- C. Hybrid
- D. Motive

Answer: A

NEW QUESTION 8

When an organization implements an SIEM solution and begins aggregating event data, the configured event sources are only valid at the time it was configured. Application modifications, patching, and other upgrades will change the events generated and how they are represented over time. What process is necessary to ensure events are collected and processed with this in mind?

- A. Continual review
- B. Continuous optimization
- C. Aggregation updates
- D. Event elasticity

Answer: B

NEW QUESTION 9

Which of the following should occur at each stage of the SDLC?

- A. Added functionality
- B. Management review
- C. Verification and validation
- D. Repurposing of any newly developed components

Answer: C

NEW QUESTION 10

Which of the following best describes SAML? Response:

- A. A standard for developing secure application management logistics
- B. A standard for exchanging authentication and authorization data between security domains
- C. A standard for exchanging usernames and passwords across devices
- D. A standard used for directory synchronization

Answer: B

NEW QUESTION 10

Of the following, which is probably the most significant risk in a managed cloud environment? Response:

- A. DDoS
- B. Management plane breach
- C. Guest escape
- D. Physical attack on the utility service lines

Answer: B

NEW QUESTION 11

Which of the following best describes data masking? Response:

- A. A method where the last few numbers in a dataset are not obscure
- B. These are often used for authentication.
- C. A method for creating similar but inauthentic datasets used for software testing and user training.
- D. A method used to protect prying eyes from data such as social security numbers and credit card data.
- E. Data masking involves stripping out all similar digits in a string of numbers so as to obscure the original number.

Answer: B

NEW QUESTION 16

You are in charge of creating the BCDR plan and procedures for your organization. Your organization has its production environment hosted by a cloud provider, and you have appropriate protections in place.

Which of the following is a significant consideration for your BCDR backup? Response:

- A. Enough personnel at the BCDR recovery site to ensure proper operations
- B. Good cryptographic key management
- C. Access to the servers where the BCDR backup is stored
- D. Forensic analysis capabilities

Answer: B

NEW QUESTION 17

Which of the following are contractual components that the CSP should review and understand fully when contracting with a cloud service provider? (Choose two.)

- A. Concurrently maintainable site infrastructure
- B. Use of subcontractors
- C. Redundant site infrastructure capacity components
- D. Scope of processing

Answer: BD

NEW QUESTION 18

A typical DLP tool can enhance the organization's efforts at accomplishing what legal task? Response:

- A. Evidence collection
- B. Delivering testimony
- C. Criminal prosecution
- D. Enforcement of intellectual property rights

Answer: A

NEW QUESTION 22

You are the security policy lead for your organization, which is considering migrating from your on-premises, legacy environment into the cloud. You are reviewing the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) as a tool for your organization. Which of the following benefits will the CSA CCM offer your organization? Response:

- A. Simplifying regulatory compliance
- B. Collecting multiple data streams from your log files
- C. Ensuring that the baseline configuration is applied to all systems
- D. Enforcing contract terms between your organization and the cloud provider

Answer: A

NEW QUESTION 27

When considering the option to migrate from an on-premises environment to a hosted cloud service, an organization should weigh the risks of allowing external entities to access the cloud data for collaborative purposes against _____. Response:

- A. Not securing the data in the legacy environment
- B. Disclosing the data publicly
- C. Inviting external personnel into the legacy workspace in order to enhance collaboration
- D. Sending the data outside the legacy environment for collaborative purposes

Answer: D

NEW QUESTION 29

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment. In order to get truly holistic coverage of your environment, you should be sure to include _____ as a step in the deployment process. Response:

- A. Getting signed user agreements from all users
- B. Installation of the solution on all assets in the cloud data center
- C. Adoption of the tool in all routers between your users and the cloud provider
- D. All of your customers to install the tool

Answer: A

NEW QUESTION 33

Which of the following is the best and only completely secure method of data destruction? Response:

- A. Degaussing
- B. Crypto-shredding
- C. Physical destruction of resources that store the data
- D. Legal order issued by the prevailing jurisdiction where the data is geographically situated

Answer: C

NEW QUESTION 35

Which of the following tools might be useful in data discovery efforts that are based on content analysis?

- A. DLP
- B. Digital Rights Management (DRM)
- C. iSCSI
- D. Fibre Channel over Ethernet (FCoE)

Answer: A

NEW QUESTION 40

Because PaaS implementations are so often used for software development, what is one of the vulnerabilities that should always be kept in mind? Response:

- A. Malware
- B. Loss/theft of portable devices
- C. Backdoors
- D. DoS/DDoS

Answer:

C

NEW QUESTION 45

You are performing an audit of the security controls used in a cloud environment. Which of the following would best serve your purpose?

Response:

- A. The business impact analysis (BIA)
- B. A copy of the VM baseline configuration
- C. The latest version of the company's financial records
- D. A SOC 3 report from another (external) auditor

Answer: B

NEW QUESTION 46

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes "cross-site scripting (XSS)." Which of the following is not a method for reducing the risk of XSS attacks? Response:

- A. Use an auto-escaping template system.
- B. XML escape all identity assertions.
- C. Sanitize HTML markup with a library designed for the purpose.
- D. HTML escape JSON values in an HTML context and read the data with JSON.parse.

Answer: B

NEW QUESTION 48

Cloud environments pose many unique challenges for a data custodian to properly adhere to policies and the use of data. What poses the biggest challenge for a data custodian with a PaaS implementation, over and above the same concerns with IaaS?

Response:

- A. Access to systems
- B. Knowledge of systems
- C. Data classification rules
- D. Contractual requirements

Answer: B

NEW QUESTION 51

Every cloud service provider that opts to join the CSA STAR program registry must complete a _____.

- A. SOC 2, Type 2 audit report
- B. Consensus Assessment Initiative Questionnaire (CAIQ)
- C. NIST 800-37 RMF audit
- D. ISO 27001 ISMS review

Answer: B

NEW QUESTION 53

What sort of legal enforcement may the Payment Card Industry (PCI) Security Standards Council not bring to bear against organizations that fail to comply with the Payment Card Industry Data Security Standard (PCI DSS)?

Response:

- A. Fines
- B. Jail time
- C. Suspension of credit card processing privileges
- D. Subject to increased audit frequency and scope

Answer: B

NEW QUESTION 57

Which of the following practices can enhance both operational capabilities and configuration management efforts?

Response:

- A. Regular backups
- B. Constant uptime
- C. Multifactor authentication
- D. File hashes

Answer: D

NEW QUESTION 58

Which of the following is a possible negative aspect of bit-splitting?

- A. Greater chance of physical theft of assets
- B. Loss of public image
- C. Some risk to availability, depending on the implementation

D. A small fire hazard

Answer: C

NEW QUESTION 61

In the cloud motif, the data processor is usually: Response:

- A. The party that assigns access rights
- B. The cloud customer
- C. The cloud provider
- D. The cloud access security broker

Answer: C

NEW QUESTION 64

Why are PaaS environments at a higher likelihood of suffering backdoor vulnerabilities?

- A. They rely on virtualization.
- B. They are often used for software development.
- C. They have multitenancy.
- D. They are scalable.

Answer: B

NEW QUESTION 66

Which of the following data sanitation methods would be the MOST effective if you needed to securely remove data as quickly as possible in a cloud environment? Response:

- A. Zeroing
- B. Cryptographic erasure
- C. Overwriting
- D. Degaussing

Answer: B

NEW QUESTION 70

You are the security manager for an online retail sales company with 100 employees and a production environment hosted in a PaaS model with a major cloud provider.

Your company policies have allowed for a BYOD workforce that work equally from the company offices and their own homes or other locations. The policies also allow users to select which APIs they install and use on their own devices in order to access and manipulate company data.

Of the following, what is a security control you'd like to implement to offset the risk(s) incurred by this practice?

- A. Regular and widespread integrity checks on sampled data throughout the managed environment
- B. More extensive and granular background checks on all employees, particularly new hires
- C. Inclusion of references to all applicable regulations in the policy documents
- D. Increased enforcement of separation of duties for all workflows

Answer: A

NEW QUESTION 75

DAST checks software functionality in _____. Response:

- A. The production environment
- B. A runtime state
- C. The cloud
- D. An IaaS configuration

Answer: B

NEW QUESTION 80

You are the security manager for a software development firm. Your company is interested in using a managed cloud service provider for hosting its testing environment. Management is interested in adopting an Agile development style.

This will be typified by which of the following traits? Response:

- A. Reliance on a concrete plan formulated during the Define phase
- B. Rigorous, repeated security testing
- C. Isolated programming experts for specific functional elements
- D. Short, iterative work periods

Answer: D

NEW QUESTION 84

A honeypot can be used for all the following purposes except _____. Response:

- A. Gathering threat intelligence
- B. Luring attackers
- C. Distracting attackers
- D. Delaying attackers

Answer: B

NEW QUESTION 85

Which of the following top security threats involves attempting to send invalid commands to an application in an attempt to get the application to execute the code? Response:

- A. Cross-site scripting
- B. Injection
- C. Insecure direct object references
- D. Cross-site request forgery

Answer: B

NEW QUESTION 87

Which of the following are considered to be the building blocks of cloud computing? Response:

- A. Data, access control, virtualization, and services
- B. Storage, networking, printing and virtualization
- C. CPU, RAM, storage and networking
- D. Data, CPU, RAM, and access control

Answer: C

NEW QUESTION 92

The Open Web Application Security Project (OWASP) Top Ten is a list of web application security threats that is composed by a member-driven OWASP committee of application development experts and published approximately every 24 months. The 2013 OWASP Top Ten list includes “sensitive data exposure.” Which of these is a technique to reduce the potential for a sensitive data exposure? Response:

- A. Extensive user training on proper data handling techniques
- B. Advanced firewalls inspecting all inbound traffic, to include content-based screening
- C. Ensuring the use of utility backup power supplies
- D. Roving security guards

Answer: A

NEW QUESTION 93

The physical layout of a cloud data center campus should include redundancies of all the following except _____. Response:

- A. Generators
- B. HVAC units
- C. Generator fuel storage
- D. Points of personnel ingress

Answer: D

NEW QUESTION 97

Which concept pertains to cloud customers paying only for the resources they use and consume, and only for the duration they are using them? Response:

- A. Measured service
- B. Auto-scaling
- C. Portability
- D. Elasticity

Answer: A

NEW QUESTION 102

What are the phases of a software development lifecycle process model? Response:

- A. Planning and requirements analysis, define, design, develop, testing, and maintenance
- B. Define, planning and requirements analysis, design, develop, testing, and maintenance
- C. Planning and requirements analysis, define, design, testing, develop, and maintenance
- D. Planning and requirements analysis, design, define, develop, testing, and maintenance

Answer: A

NEW QUESTION 104

Data labels could include all the following, except: Response:

- A. Source
- B. Delivery vendor
- C. Handling restrictions
- D. Jurisdiction

Answer: B

NEW QUESTION 107

What is the amount of fuel that should be on hand to power generators for backup datacenter power, in all tiers, according to the Uptime Institute?

- A. 1
- B. 1,000 gallons
- C. 12 hours
- D. As much as needed to ensure all systems may be gracefully shut down and data securely stored

Answer: C

NEW QUESTION 111

During which stage of the SDLC process should security be consulted and begin its initial involvement?

- A. Testing
- B. Design
- C. Development
- D. Requirement gathering

Answer: D

NEW QUESTION 113

Which of the following is not an enforceable governmental request? Response:

- A. Warrant
- B. Subpoena
- C. Court order
- D. Affidavit

Answer: D

NEW QUESTION 117

DRM solutions should generally include all the following functions, except:

- A. Persistency
- B. Automatic self-destruct
- C. Automatic expiration
- D. Dynamic policy control

Answer: B

NEW QUESTION 120

Static software security testing typically uses _____ as a measure of how thorough the testing was. Response:

- A. Number of testers
- B. Flaws detected
- C. Code coverage
- D. Malware hits

Answer: C

NEW QUESTION 125

SOX was enacted because of which of the following? Response:

- A. Poor BOD oversight
- B. Lack of independent audits
- C. Poor financial controls
- D. All of the above

Answer: D

NEW QUESTION 129

Who should be the only entity allowed to declare that an organization can return to normal following contingency or BCDR operations? Response:

- A. Regulators
- B. Law enforcement
- C. The incident manager
- D. Senior management

Answer: D

NEW QUESTION 131

Who will determine data classifications for the cloud customer?

- A. The cloud provider
- B. NIST
- C. Regulators
- D. The cloud customer

Answer: D

NEW QUESTION 136

Which of the following is not a reason for conducting audits?

- A. Regulatory compliance
- B. User satisfaction
- C. Determination of service quality
- D. Security assurance

Answer: B

NEW QUESTION 138

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment. In order to increase the security value of the DLP, you should consider combining it with _____.

Response:

- A. Digital rights management (DRM) and security event and incident management (SIEM) tools
- B. An investment in upgraded project management software
- C. Digital insurance policies
- D. The Uptime Institute's Tier certification

Answer: A

NEW QUESTION 143

The Cloud Security Alliance (CSA) publishes, the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, all of the following activity can result in data loss except _____.

- A. Misplaced crypto keys
- B. Improper policy
- C. Ineffectual backup procedures
- D. Accidental overwrite

Answer: B

NEW QUESTION 145

The use of which of the following technologies will NOT require the security dependency of an operating system, other than its own?

- A. Management plane
- B. Type 1 hypervisor
- C. Type 2 hypervisor
- D. Virtual machine

Answer: B

NEW QUESTION 150

When using transparent encryption of a database, where does the encryption engine reside? Response:

- A. At the application using the database
- B. On the instance(s) attached to the volume
- C. In a key management system
- D. Within the database

Answer: D

NEW QUESTION 155

The Transport Layer Security (TLS) protocol creates a secure communications channel over public media (such as the Internet). In a typical TLS session, what is the usual means for establishing trust between the parties?

Response:

- A. Out-of-band authentication
- B. Multifactor authentication
- C. PKI certificates
- D. Preexisting knowledge of each other

Answer: C

NEW QUESTION 157

While an audit is being conducted, which of the following could cause management and the auditors to change the original plan in order to continue with the audit?
Response:

- A. Cost overruns
- B. Impact on systems
- C. Regulatory changes
- D. Software version changes

Answer: A

NEW QUESTION 161

You are the security manager of a small firm that has just purchased a DLP solution to implement in your cloud-based production environment. Which of these activities should you perform before deploying the tool? Response:

- A. Survey your company's departments about the data under their control
- B. Reconstruct your firewalls
- C. Harden all your routers
- D. Adjust the hypervisors

Answer: A

NEW QUESTION 162

Which cloud service category brings with it the most expensive startup costs, but also the lowest costs for ongoing support and maintenance staff?
Response:

- A. IaaS
- B. SaaS
- C. PaaS
- D. DaaS

Answer: B

NEW QUESTION 163

A process for _____ can aid in protecting against data disclosure due to lost devices. Response:

- A. User punishment
- B. Credential revocation
- C. Law enforcement notification
- D. Device tracking

Answer: B

NEW QUESTION 165

In a Lightweight Directory Access Protocol (LDAP) environment, each entry in a directory server is identified by a _____.
Response:

- A. Domain name (DN)
- B. Distinguished name (DN)
- C. Directory name (DN)
- D. Default name (DN)

Answer: B

NEW QUESTION 168

Which type of cloud service category would having a vendor-neutral encryption scheme for data at rest (DAR) be the MOST important?
Response:

- A. Public
- B. Hybrid
- C. Private
- D. Community

Answer: B

NEW QUESTION 173

A bare-metal hypervisor is Type _____.
Response:

- A. 1
- B. 2
- C. 3
- D. 4

Answer: A

NEW QUESTION 177

The Cloud Security Alliance (CSA) publishes the Notorious Nine, a list of common threats to organizations participating in cloud computing. According to the CSA, what aspect of managed cloud services makes the threat of malicious insiders so alarming?
Response:

- A. Scalability
- B. Multitenancy
- C. Metered service
- D. Flexibility

Answer: B

NEW QUESTION 182

Your organization has made it a top priority that any cloud environment being considered to host production systems have guarantees that resources will always be available for allocation when needed. Which of the following concepts will you need to ensure is part of the contract and SLA? Response:

- A. Limits
- B. Shares
- C. Resource pooling
- D. Reservations

Answer: D

NEW QUESTION 186

The destruction of a cloud customer's data can be required by all of the following except _____.
Response:

- A. Statute
- B. Regulation
- C. The cloud provider's policy
- D. Contract

Answer: C

NEW QUESTION 191

The Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) addresses all the following security architecture elements except _____.
Response:

- A. Physical security
- B. IaaS
- C. Application security
- D. Business drivers

Answer: D

NEW QUESTION 193

The Cloud Security Alliance (CSA) Security, Trust, and Assurance Registry (STAR) program has _____ tiers.
Response:

- A. Two
- B. Three
- C. Four
- D. Eight

Answer: B

NEW QUESTION 198

Which one of the following is not one of the three common threat modeling techniques? Response:

- A. Focused on assets
- B. Focused on attackers
- C. Focused on software
- D. Focused on social engineering

Answer: D

NEW QUESTION 199

Which of the following are not examples of personnel controls? Response:

- A. Background checks
- B. Reference checks
- C. Strict access control mechanisms

D. Continuous security training

Answer: C

NEW QUESTION 200

Which of the following methods is often used to obscure data from production systems for use in test or development environments?

Response:

- A. Tokenization
- B. Encryption
- C. Masking
- D. Classification

Answer: C

NEW QUESTION 202

The physical layout of a cloud data center campus should include redundancies of all the following except _____.

Response:

- A. Physical perimeter security controls (fences, lights, walls, etc.)
- B. The administration/support staff building
- C. Electrical utility lines
- D. Communications connectivity lines

Answer: B

NEW QUESTION 207

Which of the following is a method for apportioning resources that involves setting maximum usage amounts for all tenants/customers within the environment?

Response:

- A. Reservations
- B. Shares
- C. Cancellations
- D. Limits

Answer: D

NEW QUESTION 208

Administrative penalties for violating the General Data Protection Regulation (GDPR) can range up to _____.

Response:

- A. US\$100,000
- B. 500,000 euros
- C. 20,000,000 euros
- D. 1,000,000 euros

Answer: C

NEW QUESTION 212

Although performing BCDR tests at regular intervals is a best practice to ensure processes and documentation are still relevant and efficient, which of the following represents a reason to conduct a BCDR review outside of the regular interval?

Response:

- A. Staff changes
- B. Application changes
- C. Regulatory changes
- D. Management changes

Answer: B

NEW QUESTION 214

Firewalls can detect attack traffic by using all these methods except _____.

Response:

- A. Known past behavior in the environment
- B. Identity of the malicious user
- C. Point of origination
- D. Signature matching

Answer: B

NEW QUESTION 216

Resolving resource contentions in the cloud will most likely be the job of the _____.

Response:

- A. Router
- B. Emulator
- C. Regulator
- D. Hypervisor

Answer: D

NEW QUESTION 218

What does nonrepudiation mean?

Response:

- A. Prohibiting certain parties from a private conversation
- B. Ensuring that a transaction is completed before saving the results
- C. Ensuring that someone cannot turn off auditing capabilities while performing a function
- D. Preventing any party that participates in a transaction from claiming that it did not

Answer: D

NEW QUESTION 219

Before deploying a specific brand of virtualization toolset, it is important to configure it according to _____.

Response:

- A. Industry standards
- B. Prevailing law of that jurisdiction
- C. Vendor guidance
- D. Expert opinion

Answer: C

NEW QUESTION 221

What is the most secure form of code testing and review? Response:

- A. Open source
- B. Proprietary/internal
- C. Neither open source nor proprietary
- D. Combination of open source and proprietary

Answer: D

NEW QUESTION 224

Which kind of SSAE audit report is a cloud customer most likely to receive from a cloud provider? Response:

- A. SOC 1 Type 1
- B. SOC 2 Type 2
- C. SOC 1 Type 2
- D. SOC 3

Answer: D

NEW QUESTION 226

In application-level encryption, where does the encryption engine reside? Response:

- A. In the application accessing the database
- B. In the OS on which the application is run
- C. Within the database accessed by the application
- D. In the volume where the database resides

Answer: A

NEW QUESTION 228

At which phase of the SDLC process should security begin participating? Response:

- A. Requirements gathering
- B. Requirements analysis
- C. Design
- D. Testing

Answer: A

NEW QUESTION 230

What are the four cloud deployment models? Response:

- A. Public, Internal, Hybrid, and Community
- B. External, Private, Hybrid, and Community
- C. Public, Private, Joint, and Community
- D. Public, Private, Hybrid, and Community

Answer: D

NEW QUESTION 235

Which of the following is not a feature of SAST? Response:

- A. Source code review
- B. Team-building efforts
- C. "White-box" testing
- D. Highly skilled, often expensive outside consultants

Answer: B

NEW QUESTION 236

Your organization is considering a move to a cloud environment and is looking for certifications or audit reports from cloud providers to ensure adequate security controls and processes.

Which of the following is NOT a security certification or audit report that would be pertinent? Response:

- A. FedRAMP
- B. PCI DSS
- C. FIPS 140-2
- D. SOC Type 2

Answer: C

NEW QUESTION 237

Data transformation in a cloud environment should be of great concern to organizations considering cloud migration because _____ could affect data classification processes/implementations.

Response:

- A. Multitenancy
- B. Virtualization
- C. Remote access
- D. Physical distance

Answer: B

NEW QUESTION 238

According to OWASP recommendations, active software security testing should include all of the following except _____ .

Response:

- A. Session initiation testing
- B. Input validation testing
- C. Testing for error handling
- D. Testing for weak cryptography

Answer: A

NEW QUESTION 239

Halon is now illegal to use for data center fire suppression. What is the reason it was outlawed? Response:

- A. It poses a threat to health and human safety when deployed.
- B. It can harm the environment.
- C. It does not adequately suppress fires.
- D. It causes undue damage to electronic systems.

Answer: B

NEW QUESTION 240

What principle must always been included with an SOC 2 report? Response:

- A. Confidentiality
- B. Security
- C. Privacy
- D. Processing integrity

Answer: B

NEW QUESTION 243

What is a form of cloud storage where data is stored as objects, arranged in a hierarchal structure, like a file tree?

Response:

- A. Volume storage
- B. Databases
- C. Content delivery network (CDN)
- D. Object storage

Answer: D

NEW QUESTION 247

All of the following are identity federation standards commonly found in use today except _____.
Response:

- A. WS-Federation
- B. OpenID
- C. OAuth
- D. PGP

Answer: D

NEW QUESTION 248

Each of the following is an element of the Identification phase of the identity and access management (IAM) process except _____.
Response:

- A. Provisioning
- B. Inversion
- C. Management
- D. Deprovisioning

Answer: B

NEW QUESTION 249

What are the phases of a software development lifecycle process model? Response:

- A. Planning and requirements analysis, define, design, develop, testing, and maintenance
- B. Define, planning and requirements analysis, design, develop, testing, and maintenance
- C. Planning and requirements analysis, define, design, testing, develop, and maintenance
- D. Planning and requirements analysis, design, define, develop, testing, and maintenance

Answer: A

NEW QUESTION 254

Which standards body depends heavily on contributions and input from its open membership base?
Response:

- A. NIST
- B. ISO
- C. ICANN
- D. CSA

Answer: D

NEW QUESTION 258

What aspect of data center planning occurs first? Response:

- A. Logical design
- B. Physical design
- C. Audit
- D. Policy revision

Answer: B

NEW QUESTION 261

What are SOCI/SOCII/SOCIII? Response:

- A. Risk management frameworks
- B. Access controls
- C. Audit reports
- D. Software development phases

Answer: C

NEW QUESTION 265

What type of software is often considered secured and validated via community knowledge?
Response:

- A. Proprietary

- B. Object-oriented
- C. Open source
- D. Scripting

Answer: C

NEW QUESTION 266

Which phase of the cloud data lifecycle also typically entails the process of data classification? Response:

- A. Use
- B. Store
- C. Create
- D. Archive

Answer: C

NEW QUESTION 267

What is a key component of GLBA? Response:

- A. The right to be forgotten
- B. EU Data Directives
- C. The information security program
- D. The right to audit

Answer: C

NEW QUESTION 271

You are the security subject matter expert (SME) for an organization considering a transition from the legacy environment into a hosted cloud provider's data center.

One of the challenges you're facing is whether the provider will have undue control over your data once it is within the provider's data center; will the provider be able to hold your organization hostage because they have your data?

This is a(n) _____ issue. Response:

- A. Interoperability
- B. Portability
- C. Availability
- D. Security

Answer: B

NEW QUESTION 275

Federation should be _____ to the users.

Response:

- A. Hostile
- B. Proportional
- C. Transparent
- D. Expensive

Answer: C

NEW QUESTION 280

Which of the following in a federated environment is responsible for consuming authentication tokens? Response:

- A. Relying party
- B. Identity provider
- C. Cloud services broker
- D. Authentication provider

Answer: A

NEW QUESTION 282

Which SSAE 16 report is purposefully designed for public release (for instance, to be posted on a company's website)?

Response:

- A. SOC 1
- B. SOC 2, Type 1
- C. SOC 2, Type 2
- D. SOC 3

Answer: D

NEW QUESTION 285

Which type of report is considered for "general" use and does not contain any sensitive information? Response:

- A. SOC 1
- B. SAS-70
- C. SOC 3
- D. SOC 2

Answer: C

NEW QUESTION 288

What is a data custodian responsible for? Response:

- A. The safe custody, transport, storage of the data, and implementation of business rules
- B. Data content, context, and associated business rules
- C. Logging and alerts for all data
- D. Customer access and alerts for all data

Answer: A

NEW QUESTION 290

All of the following methods can be used to attenuate the harm caused by escalation of privilege except: Response:

- A. Extensive access control and authentication tools and techniques
- B. Analysis and review of all log data by trained, skilled personnel on a frequent basis
- C. Periodic and effective use of cryptographic sanitization tools
- D. The use of automated analysis tools such as SIM, SIEM, and SEM solutions

Answer: C

NEW QUESTION 293

You have been tasked by management to offload processing and validation of incoming encoded data from your application servers and their associated APIs.

Which of the following would be the most appropriate device or software to consider?

Response:

- A. XML accelerator
- B. XML firewall
- C. Web application firewall
- D. Firewall

Answer: A

NEW QUESTION 297

DLP solutions typically involve all of the following aspects except _____.

Response:

- A. Data discovery
- B. Tokenization
- C. Monitoring
- D. Enforcement

Answer: B

NEW QUESTION 298

_____ can often be the result of inadvertent activity. Response:

- A. DDoS
- B. Phishing
- C. Sprawl
- D. Disasters

Answer: C

NEW QUESTION 299

An audit against the _____ will demonstrate that an organization has inadequate security controls to meet its ISO 27001 requirements.

Response:

- A. SAS 70 standard
- B. SSAE 16 standard
- C. ISO 27002 certification criteria
- D. NIST SP 800-53

Answer: C

NEW QUESTION 303

Your organization is developing software for wide use by the public. You have decided to test it in a cloud environment, in a PaaS model. Which of the following should be of particular concern to your organization for this situation?

Response:

- A. Vendor lock-in
- B. Backdoors
- C. Regulatory compliance
- D. High-speed network connectivity

Answer: B

NEW QUESTION 304

Which of the following is NOT a common component of a DLP implementation process? Response:

- A. Discovery
- B. Monitoring
- C. Revision
- D. Enforcement

Answer: C

NEW QUESTION 308

Which of the following data protection methodologies maintains the ability to connect back values to the original values? Response:

- A. Tokenization
- B. Anonymization
- C. Obfuscation
- D. Dynamic mapping

Answer: A

NEW QUESTION 313

Which of these characteristics of a virtualized network adds risks to the cloud environment? Response:

- A. Redundancy
- B. Scalability
- C. Pay-per-use
- D. Self-service

Answer: A

NEW QUESTION 315

Which of the following is not a way to manage risk? Response:

- A. Enveloping
- B. Mitigating
- C. Accepting
- D. Transferring

Answer: A

NEW QUESTION 318

The tasks performed by the hypervisor in the virtual environment can most be likened to the tasks of the _____ in the legacy environment.

Response:

- A. Central processing unit (CPU)
- B. Security team
- C. OS
- D. PGP

Answer: A

NEW QUESTION 319

Which of the following is NOT one of the security domains presented within the Cloud Controls Matrix? Response:

- A. Financial security
- B. Mobile security
- C. Data center security
- D. Interface security

Answer: A

NEW QUESTION 324

Federation allows _____ across organizations.

Response:

- A. Role replication

- B. Encryption
- C. Policy
- D. Access

Answer: D

NEW QUESTION 326

You work for a company that operates a production environment in the cloud. Another company using the same cloud provider is under investigation by law enforcement for racketeering.

Your company should be concerned about this because of the cloud characteristic of . Response:

- A. Virtualization
- B. Pooled resources
- C. Elasticity
- D. Automated self-service

Answer: B

NEW QUESTION 331

Cloud vendors are held to contractual obligations with specified metrics by:

Response:

- A. SLAs
- B. Regulations
- C. Law
- D. Discipline

Answer: A

NEW QUESTION 333

The BCDR plan/process should be written and documented in such a way that it can be used by _____. Response:

- A. Users
- B. Essential BCDR team members
- C. Regulators
- D. Someone with the requisite skills

Answer: D

NEW QUESTION 336

Which kind of SSAE report comes with a seal of approval from a certified auditor? Response:

- A. SOC 1
- B. SOC 2
- C. SOC 3
- D. SOC 4

Answer: C

NEW QUESTION 338

The nature of cloud computing and how it operates make complying with data discovery and disclosure orders more difficult. Which of the following concepts provides the biggest challenge in regard to data collection, pursuant to a legal order?

Response:

- A. Portability
- B. Multitenancy
- C. Reversibility
- D. Auto-scaling

Answer: B

NEW QUESTION 341

Devices in the cloud datacenter should be secure against attack. All the following are means of hardening devices, except:

Response:

- A. Using a strong password policy
- B. Removing default passwords
- C. Strictly limiting physical access
- D. Removing all admin accounts

Answer: D

NEW QUESTION 346

The Brewer-Nash security model is also known as which of the following? Response:

- A. MAC
- B. The Chinese Wall model
- C. Preventive measures
- D. RBAC

Answer: B

NEW QUESTION 351

During the assessment phase of a risk evaluation, what are the two types of tests that are performed? Response:

- A. Internal and external
- B. Technical and managerial
- C. Physical and logical
- D. Qualitative and quantitative

Answer: D

NEW QUESTION 354

Access should be based on _____.
Response:

- A. Regulatory mandates
- B. Business needs and acceptable risk
- C. User requirements and management requests
- D. Optimum performance and security provision

Answer: B

NEW QUESTION 359

If bit-splitting is used to store data sets across multiple jurisdictions, how may this enhance security? Response:

- A. By making seizure of data by law enforcement more difficult
- B. By hiding it from attackers in a specific jurisdiction
- C. By ensuring that users can only accidentally disclose data to one geographic area
- D. By restricting privilege user access

Answer: A

NEW QUESTION 364

Typically, SSDs are _____.
Response:

- A. More expensive than spinning platters
- B. Larger than tape backup
- C. Heavier than tape libraries
- D. More subject to malware than legacy drives

Answer: A

NEW QUESTION 367

Fiber-optic lines are considered part of layer _____ of the OSI model. Response:

- A. 1
- B. 3
- C. 5
- D. 7

Answer: A

NEW QUESTION 370

Which of the following is not a component of the of the STRIDE model? Response:

- A. Spoofing
- B. Repudiation
- C. Information disclosure
- D. External pen testing

Answer: D

NEW QUESTION 375

Proper _____ need to be assigned to each data classification/category. Response:

- A. Dollar values
- B. Metadata
- C. Security controls

D. Policies

Answer: C

NEW QUESTION 378

Cloud environments are based entirely on virtual machines and virtual devices, and those images are also in need of storage within the environment. What type of storage is typically used for virtual images?

Response:

- A. Volume
- B. Structured
- C. Unstructured
- D. Object

Answer: D

NEW QUESTION 381

Which of the following is an example of useful and sufficient data masking of the string “CCSP”? Response:

- A. XCSP
- B. PSCC
- C. TtLp
- D. 3X91

Answer: C

NEW QUESTION 384

What type of redundancy can we expect to find in a datacenter of any tier?

Response:

- A. All operational components
- B. All infrastructure
- C. Emergency egress
- D. Full power capabilities

Answer: C

NEW QUESTION 387

Which of the following would NOT be used to determine the classification of data?

Response:

- A. Metadata
- B. PII
- C. Creator
- D. Future use

Answer: D

NEW QUESTION 391

DLP solutions can aid in deterring loss due to which of the following?

Response:

- A. Randomization
- B. Inadvertent disclosure
- C. Natural disaster
- D. Device failure

Answer: B

NEW QUESTION 396

When using an Infrastructure as a Service (IaaS) solution, what is the capability provided to the customer? Response:

- A. To provision processing, storage, networks, and other fundamental computing resources when the consumer is not able to deploy and run arbitrary software, which can include operating systems and applications.
- B. To provision processing, storage, networks, and other fundamental computing resources when the provider is able to deploy and run arbitrary software, which can include operating systems and applications.
- C. To provision processing, storage, networks, and other fundamental computing resources when the auditor is able to deploy and run arbitrary software, which can include operating systems and applications.
- D. To provision processing, storage, networks, and other fundamental computing resources when the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Answer: D

NEW QUESTION 397

FM-200 has all the following properties except _____.

Response:

- A. It's nontoxic at levels used for fire suppression
- B. It's gaseous at room temperature
- C. It may deplete the Earth's ozone layer
- D. It does not leave a film or coagulant after use

Answer: C

NEW QUESTION 398

What is the major difference between authentication/authorization? Response:

- A. Code verification/code implementation
- B. Identity validation/access permission
- C. Inverse incantation/obverse instantiation
- D. User access/privileged access

Answer: B

NEW QUESTION 399

Which theoretical technology would allow superposition of physical states to increase both computing capacity and encryption keyspace? Response:

- A. All-or-nothing-transform with Reed-Solomon (AONT-RS)
- B. Quantum computing
- C. Filigree investment
- D. Sharding

Answer: B

NEW QUESTION 401

All of these are reasons an organization may want to consider cloud migration except: Response:

- A. Reduced personnel costs
- B. Elimination of risks
- C. Reduced operational expenses
- D. Increased efficiency

Answer: B

NEW QUESTION 405

Which of the following might make crypto-shredding difficult or useless? Response:

- A. Cloud provider also managing the organization's keys
- B. Lack of physical access to the environment
- C. External attackers
- D. Lack of user training and awareness

Answer: A

NEW QUESTION 408

Anonymization is the process of removing from data sets. Response:

- A. Access
- B. Cryptographic keys
- C. Numeric values
- D. Identifying information

Answer: D

NEW QUESTION 409

Which ISO/IEC standards set documents the cloud definitions for staffing and official roles? Response:

- A. ISO/IEC 27001
- B. ISO/IEC 17788
- C. ISO/IEC 17789
- D. ISO/IEC 27040

Answer: B

NEW QUESTION 411

An audit against the _____ will demonstrate that an organization has a holistic, comprehensive security program. Response:

- A. SAS 70 standard

- B. SSAE 16 standard
- C. SOC 2, Type 2 report matrix
- D. ISO 27001 certification requirements

Answer: D

NEW QUESTION 416

Which of the following is a risk that stems from a virtualized environment? Response:

- A. Live virtual machines in the production environment are moved from one host to another in the clear.
- B. Cloud data centers can become a single point of failure.
- C. It is difficult to find and contract with multiple utility providers of the same type (electric, water, etc.).
- D. Modern SLA demands are stringent and very hard to meet.

Answer: A

NEW QUESTION 421

Which of the following types of software is a Type 2 hypervisor dependent on that a Type 1 hypervisor isn't? Response:

- A. VPN
- B. Firewall
- C. Operating system
- D. IDS

Answer: C

NEW QUESTION 422

Who operates the management plane? Response:

- A. Regulators
- B. End consumers
- C. Privileged users
- D. Privacy data subjects

Answer: C

NEW QUESTION 425

Security best practices in a virtualized network environment would include which of the following? Response:

- A. Using distinct ports and port groups for various VLANs on a virtual switch rather than running them through the same port
- B. Running iSCSI traffic unencrypted in order to have it observed and monitored by NIDS
- C. Adding HIDS to all virtual guests
- D. Hardening all outward-facing firewalls in order to make them resistant to attack

Answer: A

NEW QUESTION 430

Which kind of SSAE audit reviews controls dealing with the organization's controls for assuring the confidentiality, integrity, and availability of data? Response:

- A. SOC 1
- B. SOC 2
- C. SOC 3
- D. SOC 4

Answer: B

NEW QUESTION 432

With cloud computing crossing many jurisdictional boundaries, it is a virtual certainty that conflicts will arise between differing regulations. What is the major impediment to resolving conflicts between multiple jurisdictions to form an overall policy?

Response:

- A. Language differences
- B. Technologies used
- C. Licensing issues
- D. Lack of international authority

Answer: D

NEW QUESTION 437

Managed cloud services exist because the service is less expensive for each customer than creating the same services for themselves in a legacy environment. Using a managed service allows the customer to realize significant cost savings through the reduction of _____.

Response:

- A. Risk
- B. Security controls
- C. Personnel
- D. Data

Answer: C

NEW QUESTION 441

What is the term used to describe loss of access to data because the cloud provider has ceased operation? Response:

- A. Closing
- B. Vendor lock-out
- C. Vendor lock-in
- D. Masking

Answer: B

NEW QUESTION 442

In general, a cloud BCDR solution will be _____ than a physical solution. Response:

- A. Slower
- B. Less expensive
- C. Larger
- D. More difficult to engineer

Answer: B

NEW QUESTION 445

What is one of the benefits of implementing an egress monitoring solution? Response:

- A. Preventing DDoS attacks
- B. Inventorying data assets
- C. Interviewing data owners
- D. Protecting against natural disasters

Answer: B

NEW QUESTION 450

Software-defined networking (SDN) is intended to separate different network capabilities and allow for the granting of granular configurations, permissions, and features to non-network staff or customers. Which network capability is separated from forwarding of traffic? Response:

- A. Routing
- B. Firewalling
- C. Filtering
- D. IPS

Answer: C

NEW QUESTION 453

Which of the following is perhaps the best method for reducing the risk of a specific application not delivering the proper level of functionality and performance when it is moved from the legacy environment into the cloud? Response:

- A. Remove the application from the organization's production environment, and replace it with something else.
- B. Negotiate and conduct a trial run in the cloud environment for that application before permanently migrating.
- C. Make sure the application is fully updated and patched according to all vendor specifications.
- D. Run the application in an emulator.

Answer: B

NEW QUESTION 454

It is important to include _____ in the design of underfloor plenums if they are also used for wiring. Response:

- A. Mantraps
- B. Sequestered channels
- C. Heat sinks
- D. Tight gaskets

Answer: D

NEW QUESTION 459

Setting thermostat controls by measuring the temperature will result in the _____ highest energy costs. Response:

- A. Server inlet

- B. Return air
- C. Under-floor
- D. External ambient

Answer: B

NEW QUESTION 463

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

CCSP Practice Exam Features:

- * CCSP Questions and Answers Updated Frequently
- * CCSP Practice Questions Verified by Expert Senior Certified Staff
- * CCSP Most Realistic Questions that Guarantee you a Pass on Your First Try
- * CCSP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The CCSP Practice Test Here](#)